10-22-04

IFW

tCustomer No.: 07278

Docket No.: 20193/0201102-US0

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Wieland Fischer et al.

Serial No.: 10/825,625

Filed: April 15, 2004

For: METHOD AND APPARATUS FOR PROTECTING AN EXPONENTIATION CALCULATION BY MEANS OF THE CHINESE REMAINDER THEOREM (CRT)

October 21, 2004

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Information Disclosure Statement is submitted in accordance with 37 C.F.R. 1.97, 1.98, and it is requested that the information set forth in this statement and in the listed documents be considered during the pendency of the above-identified application, and any other application relying on the filing date of the above-identified application or cross-referencing it as a related application.

1. This IDS should be considered, in accordance with 37 C.F.R. 1.97, as it is filed:(Check one of the boxes A-D)

[]A. Within three months of the filing date of the above-identified national application or within three months of the entry into the national stage of the above-identified international application.

[X] B. before the mailing date of a first office action on the merits, or a first office action after filing a request for continued examination.

[] C. after (A) and (B) above, but before the mailing date of a final rejection, a notice of allowance, or any other action that closes prosecution, and Applicants have made the necessary statement in box "i" below or paid the necessary fee in box "ii" below.

(check one of the boxes "i" and "ii" below:)

[] i. Counsel states that, upon information and belief, each item of information listed herein was either (a) cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this IDS; or (b) was not cited in a communication from a foreign patent office in a counterpart foreign application and, to the knowledge of undersigned after making reasonable inquiry, was not known to any individual designated in 1.56(c) more than three months prior to the filing of this IDS.

[] ii. A check for the fee set forth in 1. 17(p), presently believed to be $180, is enclosed.

[] D. after (A), (B) and (C) above, but before payment of the issue fee: Counsel states that, upon information and belief, each item of information listed herein was either (i) cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the IDS; or (ii) was not cited in a communication from a foreign patent office in a counterpart foreign application and, to the knowledge of the undersigned after making reasonable inquiry, was not known to any individual designated in 1.56(c) more than three months prior to the filing of this IDS.

[] i. A check for the fee set forth in 1.17 (p), presently believed to be $180, is enclosed.

2. In accordance with 37 C.F.R. 1.98, this IDS includes a list (e.g., form PTO/SB/08) of all patents, publications, or other information submitted for consideration by the office, either incorporated into this IDS or as an attachment hereto. A copy of each document listed is attached, except as explained below.

(check boxes A, B and/or C and fill in blanks, if appropriate.).

[] A. Pursuant to the Notice issued by the United States Patent and Trademark Office dated July 11, 2003 waiving the requirements of 37 C.F.R. § 1.98(a)(2)(i), a copy/copies of the United States Patent on PTO/SB08 is/are not being submitted.

[] B. Document(s) _____ is (are) deemed substantially cumulative to document(s) _____ , and, in accordance with 1.98(c), only a copy of each of the latter documents is enclosed.

[] C. Certain documents were previously cited by or submitted to the Office in the following prior applications, which are relied upon under 35 U.S.C. 120:

[SERIAL NO. & FILING DATE].

Applicant identifies these documents by attaching hereto copies of the forms PTO-892 and PTO/SB08 from the files of the prior application(s) or a fresh PTO/SB/08 listing these documents, and request that they be considered and made of record in accordance with 1.98(d). Per 37 CFR 1.98(d), copies of these documents need not be filed in this application.

[X] 3. Documents 4-7 and 15 are not in the English language. In accordance with 1.98(c), Applicant states:

- [X] An English abstract of documents 4, 5, 6 and 7 (or of the pertinent portions thereof), or a copy of each corresponding English-language patent or application is enclosed.
- [] A concise explanation of the relevance of document(s) _____ is found in the attached search report (see MPEP § 609 A(3)x).
- [] A concise explanation of the relevance of document(s) _____ is set forth as follows: [Insert concise explanation of relevance]
- [] A concise explanation of the relevance of document(s) _____ can be found on page(s) _____ of the specification.
- [X] A concise explanation of document 15 can be found on the attached sheet.

[] 4. No explanation of relevance is necessary for documents in the English language (see MPEP § 609 A(3)).

[] 5. Other information being provided for the examiner's consideration follows: [A/An _____ Search Report, dated_____, which issued during the prosecution of _____Application No._____ which corresponds to the present application.]

6. In accordance with 37 C.F.R. 1.97(g) and (h), the filing of this IDS should not be construed as a representation that a search has been made or that information cited is, or is considered to be, material to patentability as defined in §1.56 (b), or that any cited document listed or attached is (or constitutes) prior art. Unless other-wise indicated, the date of publication indicated for an item is taken from the face of the item and Applicant reserves the right to prove that the date of publication is in fact different.

CROSS REFERENCE UNDER 37 C.F.R. §1.78 TO RELATED APPLICATIONS

Pursuant to 37 C.F.R. § 1.78, Applicant notes that the above-identified patent application may be related to the following U.S. Patent Applications:

(1) U.S. Patent Application Serial No _____, filed _____.

Early and favorable consideration is earnestly solicited.

Respectfully submitted,

October 21, 2004

FLYNN BARRISON (53,970)

Laura C. Brutman
Registration No. 38,395
Attorney for Applicant(s)

DARBY & DARBY P.C.
805 Third Avenue
New York, N.Y. 10022
(212) 527-7700

PTO/SB/08a/b (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	10/825,625-Conf. #7860
Filing Date	April 15, 2004
First Named Inventor	Wieland Fischer
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	20193/0201102-US0

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number: Number-Kind Code[2] (*if known*)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1	US-6,092,229-B1	07-18-2000	Boyle et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document: Country Code[3]-Number[4]-Kind Code[5] (*if known*)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
	2	EP-0 743 774-A2	11-20-1996	Certicom Corp.		
	3	EP-0 872 795-A1	10-21-1998	Mykotronx, Inc.		
	4	DE-42 34 165-C1	03-03-1994	Detecon GmbH		
	5	DE-197 25 167-A1	12-17-1998	Utimaco Safeware AG		
	6	DE-199 61 838-A1	07-05-2001	SCM Microsystems GmbH		
	7	EP-0 621 569-B1	07-14-1999			

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	8	Wu, Chung-Hsien, et al., "RSA Cryptosystem Design Based on the Chinese Remainder Theorem", IEEE, 2001, pp. 391-395.	
	9	Comba, P.G., "Exponentiation cryptosystems on the IBM PC", IBM Systems Journal, 1990, Vol. 29, No. 4, pp. 526-538.	
	10	Shand, M., et al., "Fast Implementations of RSA Cryptography", 11th Symposium on Computer Arithmetic, June 29-July 2, 1993, pp. 252-259.	
	11	Grossshadl, Johann, "High-Speed RSA Hardware Based on Barret's Modular Reduction Method", 2000, pp. 191-203.	
	12	Quisquater, J., et al., "Fast Decipherment Algorithm For RSA Public-Key Cryptosystem", Electronics Letters, October 1982, Vol. 18, No. 21, pp. 905-907.	
	13	Bao, F., et al., "Breaking Public Key Cryptosystems on Tamper Resistant Devices in the Presence of Transient Faults", Proceedings of the 5th Workshop on Secure Protocols, LNCS 1361, April 7-9, 1997, pp. 115-124.	
	14	Klima, Vlastimil, et al., "Attack on Private Signature Keys of the OpenPGP format, PGP TM programs and other applications compatible with OpenPGP", March 22, 2001, pp. 1-20.	
	15	Rankl, Wolfgang, et al., "Handbuck der Chipkarten", pp. 138-139.	
	16	Boneh, Dan, et al., "On the Importance of Eliminating Errors in Cryptographic Computations", Journal of Cryptology, 2001, Vol. 14, pp. 101-119.	
	17	Shamir, A., "How to check modular exponentiation", Oral publication.	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English language Translation is attached.

Examiner Signature		Date Considered	

Application No. (if known): 10/825,625 Attorney Docket No.: 20193/0201102-US0

Certificate of Express Mailing Under 37 CFR 1.10

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail, Airbill No. in an envelope addressed to:

EV 367699741US

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

on October 21, 2004
Date

A. Stantini
Signature

A. Stantini
Typed or printed name of person signing Certificate

Registration Number, if applicable

Telephone Number

Note: Each paper must have its own certificate of mailing, or this certificate must identify each submitted paper.

Information Disclosure Statement (4 pages)
PTO SB/08 (1 page)
16 Documents
Return Postcard